The Convergence of Military and Civil Approaches to Information Security?

(February 2000)

Robert Rowlingson
(Principal Scientist)

Defence and Evaluation Research Agency,
Woodward Building, DERA Malvern
St Andrews Road, Malvern
Worcs., WR14 3PS, UK

Introduction

The motivation for this paper is the about-turn that defence computing went through with open systems interconnection (OSI) and Ada. Defence specific products and bespoke development were discarded as the cost-benefits of mainstream COTS systems became far superior. This paper shows that a similar situation is developing in information security (infosec) and suggests that the defence approach to security may need to adapt if it is to benefit from the rapidly growing commercial market.

Civil Trends in Information Security

In recent years, the civil market for information security technologies has grown dramatically. The increasing requirement for information security arises from the need to mitigate the risks involved with:

- **E- commerce**: use of the internet both for business-to-business (B2B) and business-to-consumer (B2C) sales;
- **Mobility**: support for tele-working and mobile users;
- **Extranets**: the need to establish rich inter-connectivity with business partners (as well as customers and suppliers);
- **Knowledge management**: the increasing recognition of the importance and value of information in the 'knowledge economy'.

These drivers are forcing IT departments to develop and implement security policies that go beyond the boundary of the company. Internal systems can no longer be isolated from the outside world. Critical sources of company information such as the data warehouse must be made available to staff, partners, customers, potential customers and collaborators [1]. The pressure is on all companies to exploit the internet and to accept the risk that connecting to a public network inevitably carries. Lack of security and trust are the greatest inhibitors of the commercial use of the internet [2, 3]. Everyone accepts the need to practice 'safe hex'!

Anecdotal evidence of the relative importance of various infosec issues is indicated by the 'Top 5 Information Security Concerns for Corporations in 1999' [4].

1) Ability of current infrastructure to support e-commerce activities;
2) Implementing remote access without compromising the security of the corporate network;
3) 'Insider' attacks against corporate systems;
4) The extension of networks to support business partner connections;
5) Encryption and key management technology for customer facing systems.

Consequently companies are developing security policies; purchasing products such as firewalls and intrusion detection systems; procuring services such as penetration testing and security auditing; and training their staff in information security. In short, they are doing many of the things that defence has considered as essential for many years. This is driving massive growth in the information security market - in 2001 the internet security business is predicted to be worth $7bn with an annual growth rate in the whole information security industry of 65% [5].

Defence Trends and Information Security

The trend towards more joint and coalition operations means the ability to federate systems is essential. There is also a growing need to work with Non-Governmental Organisations as well as within the Government Secure Intranet (GSI). The Smart Procurement Initiative (SPI) has highlighted the need to use electronic commerce and for close partnerships with industry. The doctrine of 'information superiority' has brought the role of information in military operations to the fore. All four commercial drivers: e-commerce, mobility, extranets and knowledge management, are thus also applicable to the defence sphere. There is a *prima facie* case that the civil approach to security is becoming increasingly relevant to defence.

Comparing Defence and Civil Infosec

It would be comforting to believe that the massive civil investment in infosec and developments in areas like cryptography mean effective security will become easier. However some commentators believe that it is likely to get worse before it gets better. It is safe to assume that all systems can be successfully attacked in some way – probably in a way unexpected by the designers and with unexpected consequences. Defenders have to defend every vulnerability, whereas attackers have only to find one weak spot. Complex software will always have bugs

Paper presented at the RTO IST Symposium on "Commercial Off-the-Shelf Products in Defence Applications "The Ruthless Pursuit of COTS"", held in Brussels, Belgium, 3-5 April 2000, and published in RTO MP-48.

and features that pre-dispose it to security vulnerabilities. Security is dynamic and both risks and counter-measures are evolving rapidly. What does this mean for the convergence of military and civil approaches to infosec?

The military's ability to exploit the market will depend on whether the nature and level of protection it requires for information will be supportable using civil products and services. The requirements will depend on the perceived risks that security will be compromised, and the impact that a compromise has on the organisation's mission - in the case of defence to defend, in the case of industry to make profits. In both cases there is a trade-off between the protection of information and the sharing of information. Sharing is deemed to have a benefit; protection a cost. Thus at the heart of information security is a cost-benefit analysis which we can understand using four basic components of information security:

- Information is subject to various forms of potential **compromise**. A compromise is a breakdown in information security. It occurs whenever some property of information that needs to be preserved, is lost; examples include loss of confidentiality, integrity, availability, utility and authenticity;
- There is a **risk** of a given loss taking place. A risk is the chance that a potential compromise will actually occur;
- A loss will have some **impact** on the organisation. Impact is the cost to the organisation caused by a security compromise;
- An organisation can protect its information from compromise, by controlling the ways it shares information, with the support of carefully selected security controls known as **counter-measures**. A counter-measure is any action taken to reduce the risk, or potential impact of, an information security compromise.

It is the objective of information security to apply appropriate, cost-effective, counter-measures in order to reduce, the risk and impact of compromise, without undue effect on system usability. There is no universal agreement over the exact meanings of many terms in information security, however these components can support a discussion of how the defence requirements compare with the civil sector.

Compromise

The principal security concern of defence is to preserve the confidentiality of its information. It is now clear that these concerns are shared by industry which is giving a much higher priority to confidentiality than it has in the past. Companies in the US are estimated to be losing $250Bn annually to information thieves. Over a 17 month period some 1100 documented incidents of intellectual property theft were identified worth an estimated $44Bn [5, 6]. Trusted insiders are widely acknowledged as the single greatest threat to corporate information.

Risk

In providing a secure system, it is imperative that security measures should be designed to counter the most likely and most damaging causes of compromise. These can be characterised by [7]:

- accidents caused by the legitimate users of the system;
- the actions of a traitor, i.e. a legitimate user betraying the trust placed in them;
- trojan horse software unwittingly invoked by a legitimate user, thereby allowing illegal users access to the legitimate business processes;
- someone exploiting an implementation flaw or weakness in the security system;
- legitimate users failing to follow security operating procedures.

Risk assessment is the starting point for all security decisions and goes hand-in-hand with assessment of the potential impact. However we cannot precisely quantify risk - it is a probability which depends on many unknowns and unknowables. Formal quantitative risk assessment is prone to errors.

Companies are good at assessing and taking business risks. They make money by accepting and managing risks better then their competitors and this includes infosec risks. They take a pragmatic approach to the cost-benefit analysis, preferring skilled judgement to risk minimisation or analytical risk assessment. They are unlikely to favour the rigorous, quantitative approach used in defence.

In business, IT is purchased first and foremost for a given business purpose; security is then retrofitted to the system. In contrast the defence approach to security is based on a prescribed set of engineering principles; an analysis of how close a given system conforms to those principles and an evaluated assurance level. These principles tacitly assume a 'clean sheet' that can be designed from the ground up with security in mind. 'Security by design' is acknowledged as the best way to achieve security but as an approach it is fundamentally different to the civil sector.

The defence approach also contains a 'standard' attitude to risk. This has the benefit of consistency and accountability. However, the use of a pre-defined set of rules, enforced at system installation, is a significant restraint on flexibility and responsiveness by system owners. In the worst case, users may feel that security is not their problem, as it has already been addressed by a separate group of staff responsible for accreditation. As there is no guarantee that security adopted at the beginning of a project is suitable at a later date, security must be considered throughout the lifetime of a system.

The causes of compromise described above are made up of threats and vulnerabilities.

Threat

A threat is an action or event that can cause an information compromise. There are five broad classes of threat agents – criminals, terrorists, employees, other outsiders (e.g. former employees) and competitors (the enemy). Threat agents are either internal or external to an organisation; structured (i.e. organised in some way) or unstructured. To pose a threat, someone must possess the Skills, Knowledge, Resources, Authority and Motives (SKRAM) necessary to cause a compromise [8].

An area where the threat (or SKRAM) is increasing rapidly is hacking. Hacking is seen as 'cool' and in some circumstances is profitable. It is also becoming more widespread, as hacking tools are published on the web and many people start to experiment with them. However most of these 'script kiddies' are easy to repulse by competent system managers. The tools they naively employ are also useful to system managers to test and protect their networks. For example, L0phtCrack[1] is a password guesser. One NT administrator found 85% of his office's passwords in 20 minutes, all but two in a day [9]. It can and should be used by defenders to check that users are choosing passwords which are difficult to guess. Another common hacking technique is known as packet sniffing - the providers of L0phtCrack have also published a packet sniffer detector (a stealth packet sniffer is also available!). Hackers may be threats but their techniques often provide potentially useful countermeasures.

Vulnerabilities

A vulnerability is an inherent weakness in a system that may allow a threat to cause an information compromise. The critical issue for defence is that if it uses COTS software, it exposes itself to vulnerabilities that are well-known to potential attackers. The alternative approach is to develop non-COTS software and rely on 'security by obscurity', in other words to assume that as mainstream users and hackers do not use the software they cannot find any vulnerabilities to exploit. Indeed, many vulnerabilities are found in COTS technologies because users find bugs and exploitable 'features', and many people (good and bad) look for such vulnerabilities.

COTS software is potentially more secure than 'obscured' software in three ways. Firstly, the vulnerabilities that are easiest to find can be found and fixed; secondly, there is a short window of opportunity for an attacker to target a given system because fixes are released quickly and widely notified; and lastly, the chance that a system has unknowingly been compromised is less, as someone else using the same system may discover it first). To make this approach work, system vulnerabilities need to be monitored and disseminated – the role of a CERT (Computer Emergency Response Team) and patches and work-arounds must be quickly applied - the role of a system manager. Thus the COTS approach applies throughout the lifecycle and is less 'all or nothing' than a system that has some dependency on security by obscurity.

If the security of a system depends on it's obscurity then if that obscurity is ever compromised, and we may not actually know if it is, all bets are off. Further problems arise as such systems are generally not designed for rapid patching and updates, as with COTS. In some cases if a vulnerability was ever found, it would be very difficult to correct in the field. Examples of the failure of 'security by obscurity' in the civil sector are commonplace:

- The U.S. digital cellular companies created their own proprietary cryptography; some algorithms were made public without their consent [10]; once public they were broken. Now the industry is considering public algorithms to replace them;
- The security of Digital Versatile Disks (DVD) relies on the confidentiality of the code that performs the decryption in a DVD player. However, unencrypted code was found and this enabled the system to be reverse-engineered and compromised[2]. The software to do this was then posted on the web [11].
- Microsoft introduced Point-to-Point Tunnelling protocol (PPTP) as its Virtual Private Network (VPN) technology (competing with the internet standard IPSEC that has gone through rigorous public review). Microsoft fielded PPTP in Windows NT and 95, and published their protocols. In 1998 various flaws were published and Microsoft quickly posted a series of fixes (which were evaluated and found improved, but still flawed) [10].

These events also suggest that if security vulnerabilities are found in the COTS it procures then defence has a good chance of having them corrected by suppliers. (This is completely different from the case of functionality, where defence has very little influence over suppliers). However it is necessary to make the vulnerability known to the supplier and this would clearly involve some risk. Indeed this could be compounded by the fact that many suppliers appear to respond much more quickly to flaws that are in the public domain rather than those that have been communicated privately. It can seriously tarnish their reputation if they are seen to respond slowly to a security problem in a security product.

[1] The word L0phtCrack incorporates several techniques for choosing difficult-to-guess passwords.

[2] The key size had been limited by US export law but a brute force attack was not used, nor was any encryption algorithm broken – failure was due to a reliance on the confidentiality of an algorithm.

Impact

Defence has a very effective and well-developed system for evaluating impact – protective-marking. The classification of a document is a direct indication of the impact its loss of confidentiality would have on national defence. However the civil sector does not see that a detailed and rigorous multi-level classification scheme can be cost-effective. There is rarely a clear business case to undertake and maintain an information classification regime and the necessary vetting of staff. Furthermore, classification is of little use in understanding the impact of a loss of integrity or availability [12]. This is despite the benefits that such an approach offers, such as a better understanding of where to invest security resources and a visible reminder to staff to take appropriate care. Defence cannot look to COTS for support for multi-level document labelling schemes although simple support for 'need-to-know' type labels such as commercial-in-confidence, may be of interest to the civil sector and thereby provide a market for an appropriate COTS product.

Countermeasures

Thanks to the game of 'catch-up' between infosec defence and attack, counter-measure technology is a fast-moving field. The size of the market, and more importantly, the size of the e-business market it enables, suggests that it will continue to evolve rapidly towards the corporate mainstream. Much of it is highly relevant to defence. This section illustrates the proliferation of COTS technologies [13, 14]:

Biometrics

Biometrics refers to the ability of an attribute like a fingerprint to uniquely identify an individual. Techniques such as voice identification; fingerprints; facial, retina and iris recognition; and hand geometry are being pursued. High demand and improving technology is causing a rapid drop in price for usable biometric technologies.

Encryption

Encryption technology is a rapidly developing area in the civil sector which, until the publication of the concept of public key cryptography in 1976 (Diffie-Hellman) was almost the sole preserve of the defence sector [15]. Nowadays, innovative products are emerging in applications such as secure email, e-commerce, internet banking, copyright protection in digital media, cellular telephony and the like. These include:

- Certigrams - 2-dimensional representations of encrypted information;
- Hushmail (a browser-based email system like Hotmail but where the email on the mail server and all interactions with it are encrypted);
- Elliptic curve cryptography - a form of public key cryptography with a smaller key size and faster implementations than other public key algorithms.

In the past, defence has focussed on providing strong encryption algorithms to prevent enemy decoding. The civil sector recognises that a secure system is only as secure as its weakest link. Most threats will not attempt to crack encryption using code-breaking – it is far easier to steal keys or bribe people. The critical civil sector requirement is therefore for secure cryptosystems. The civil sector is also developing strong algorithms such as the Advanced Encryption Standard (AES). This is an open competition and civil cryptographers are attempting to find flaws in the competitors.

Encryption is becoming something of a 'silver bullet' in the civil sector. Despite its obvious potential and diverse applicability there remain many drawbacks:

- A perfect cryptosystem is no more achievable than perfect security;
- Encrypting everything everywhere is complex and costly;
- There are a variety of disparate algorithms, approaches and products;
- Encryption does little to counter trojan horse attacks;
- An attacker can use encryption to hide stolen information, malicious code, etc.;
- Encryption still requires identification for secure transactions;
- Encryption is a complex application - users can easily make serious mistakes.

The most worrying aspect of the widespread use of cryptography is that it may actually give users, and system owners, a false sense of security.

Snoopware

Snoopware is a colloquialism for software which monitors user behaviour and communciations[3] such as email; keystrokes; time and date of activities; name of program being used etc.. Snoopware is the internal analogue of intrusion detection – it has the potential to detect traitors and spot how accidental compromises occur.

Content Checking

Content checkers analyse information or 'content' passing in or out of a system. For example, outbound checks for words in email which suggest information is classified; inbound checks to block executables. Companies are using this software extensively to protect against their liability for the actions of their employees, who might send libellous or discriminatory emails. The difficulty is that little information is sent in plain ASCII text and checkers need to decompose attachments in compressed, encrypted or obscure formats, to apply a content policy to as much data as possible.

[3] Clearly there are many privacy issues concerning the use of such software.

Firewalls
Firewalls are the mainstay of network security. They form the first line of defence against network based attack. The main purpose of a firewall is to police a network access policy by examining and evaluating network traffic as it passes between networks. This strategic position means that as well as keeping the bad guys out they also enable the right connections to be made, for example to support the secure mediation of e-commerce. Consequently they are designed to let information through as much as to keep it out, acting like traffic lights to the various network protocols.

Vulnerability Scanners
Vulnerability scanners are tools that test a system against a database of known vulnerabilities. They have emerged as a key hacker tool but are also important for a sound defence. Several tools have initially been published on the web and then commercialised. Recently they have been used to probe internet systems, such as web and mail servers, to find whether they were running software with known security vulnerabilities. The Internet Auditing Project scanned almost every internet server and found several hundred thousand vulnerabilities. [16]

Intrusion Detection
Intrusion detection tools monitor access, attempted access and other interactions within and between networks. Basically they attempt to identify possible malicious behaviour, for example: repeated password guessing or non-standard attempts to create new users. They may monitor network traffic in real-time, or analyse audit logs off-line. Most products on the market look for specific patterns in user activity and tend to be inflexible. Some systems are now attempting to use heuristics and artificial intelligence techniques to improve detection rates and reduce false alarms.

Malware Protection
Malware is the generic name for harmful software such as viruses and trojan horses. Most anti-virus tools work by recognising 'signatures' of known viruses and require regular updates of new virus signatures. This means they may overlook new viruses, as the 'Melissa' outbreak demonstrated. Other malware protection software includes integrity checkers, which check that the system configuration has not been altered, and release sanctions, which ensure information is only released with user approval.

Information Security Management

Technology *per se* is of little use in information security if not backed up by policies and well-managed processes. Several civil standards are relevant:

- A Code of Practice for Information Security Management (BS7799-1:1999) [17] - aims to provide common, best practice guidance to enable an organisation to implement appropriate information security, and to facilitate inter-company trading by providing confidence in the security of shared information. It is an ISO 9001-like system in that it requires an organisation to 'say' what it does and 'show' that it does it, without specifying what the actual processes should be;
- System Security Engineering Capability Maturity Model (CMM) from SEI - a variant of the well-known software engineering CMM;
- Guidelines for the Management of IT security (GMITS ISO/IEC 13335) - provides a basis for an organisation to develop and enhance its security architecture and a means to establish commonality between organisations.

What appears to be missing is some way to allow one organisation to 'know' how secure another one actually is. This might be met by a composable security system description. In the world of inter-connected e-business this is a gaping hole.

Conclusions

In areas of IT where defence and civil sector requirements have a significant degree of overlap, defence has been persuaded that in order to keep pace with technology developments it must adopt the civil sector approach. This paper has highlighted the trends demonstrating that information security is heading in this direction. This implies that COTS technologies will become the default for many defence information security applications and that the defence and civil sector approaches to information security will converge. Note that COTS are not universal solutions. The highest classified information required in defence has no counterparts in the civil sector and there is unlikely to be any alternative to restricting such information to paper or isolated, physically-protected systems. However, there are a number of difficult issues which defence now faces:

- *How to manage risk more pragmatically*: Pragmatic risk management requires the application of judgement. This can be supported by a coherent traceable argument from high level policy, through individual project requirements and on to design, implementation and operation. Since perfect security is impossible there is always a degree of residual risk. The current approach does not manage it well because, unlike the civil sector, it does not accept it exists.

- *How to reduce its dependence on security by obscurity*: Defence systems are being developed that have a significant element of reliance on security by obscurity. However, if the obscurity is ever compromised (and it may not be clear if it has) an attacker may find the one vulnerability required. Attempting to fix a significant vulnerability in the field may be totally impractical.

- *How to gain confidence in the software it procures without a large formal assurance overhead*: The concept of assurance is not widely accepted in the civil sector[4]. Evaluations do not generally find common vulnerabilities, such as buffer overflows [18] and denial of service attacks [19]. Vendors are not prepared to jeopardise time-to-market for assurance, given their customers do not request it. There is a limited range of evaluated products. Frequently, only parts of the security functionality are assured. Until these drawbacks are overcome, assurance is unlikely to have a major impact in the market. Governments may need to re-define their approach, for example by recognising that mass use of software confers a certain degree of assurance and that open source software allows the requisite code inspection.

- *How to manage security on the timescales of the civil sector*: Information security is not static. If a system is 'secure' today it probably isn't tomorrow. It is dangerous to assume that a system, and its mode of operation, can be accredited at installation time as 'secure'. The civil view is that systems must always be considered insecure and that continual monitoring and rapid patching is essential.

- *How to address document marking*: The civil sector does not currently see a business case for the use of multi-level security and related document labelling. It is highly unlikely that COTS products will emerge to fulfil defence requirements. There are several alternatives: make labelling software available as a toolkit to promote its integration into defence systems; mandate a government labelling product; use encryption to manage security levels throughout its systems; or rely on informal separation and user conformance.

- *How to manage secure systems federation*: The internet demonstrates the effectiveness of a distributed, rather than a centralised, approach to systems federation. Currently this works for a simple trust model, namely trust nothing that you do not control. There is likely to be a requirement for techniques to manage more complex systems federation and secure service mediation for e-business.

In some of these aspects, such as the protection of information at the highest levels and the use of protectively-marked documents, it is unlikely that defence will find commercial solutions. In other areas, such as assurance, careful consideration is required to manage the mismatch between the defence and civil approaches. Finally, in its approach to issues such as risk assessment, static security, and security by obscurity, there are no technical reasons why the civil approach could not be used.

[4] Case law could overturn this view by ruling that 'due care' requires the use of evaluated products. However this is not likely in the short term.

References

[1] Turning Security On Its Head, The Forrester Report V13 (2), January 1999

[2] Nov 12 1999: A joint survey from @dtech and Talk City "The World Wide Internet Opinion Survey", found 83 percent of respondents had made an impulse buy online... and 45 percent cited security as the main deterrent.

[3] Security Portal Nov 15th, http://www.securityportal.com

[4] Bellcore/GlobalIntegrity's SecureComm 98 conference

[5] Computer Security Issues and Trends, 1999 CSI/FBI Computer Crime and Security Survey.

[6] Who's stealing your information? Dorothy E. Denning, http://www.infosecuritymag.com/apr99/cover.htm

[7] Interim Security Domain Modelling Guidance, Version 2.1, October 1999, DERA/CIS/CIS3/CR990148, K J Hughes

[8] Fighting Computer Crime, A New Framework for Protecting Information. Donn B.Parker, John Wiley and sons, 1998

http://www.washingtonpost.com/wp-dyn/business/A18205-1999Nov3.html

[9] http://www.lopht.com

[10] Cryptogram, September 1999, http://www.counterpane.com

[11] Hackers Unlock DVD Code, November 4th, Washington Post,

[12] CSI Roundtable: experts discuss the role of data classification now and in the future. Richard Power, Computer Security Institute Quarterly, V14 (2)

[13] A Guide to Security Technologies – A Primer for IT Professionals, RSA security

[14] Information Protection Fundamentals, Thomas R. Peltier, http://www.gocsi.com/ip.htm

[15] Applied Cryptography, Bruce Schneier. Wiley 1998

[16] The Internet Auditing Project http://www.securityfocus.com/templates/forum_message.html?forum=2&head=32&id=32

[17] The Revised Version of BS7799 – So What's New? Chris Pounder, Computers and Security V18 (1999) pp307-311

[18] Study says "buffer overflow" is most common security bug, www.cnet.com

[19] Computer Security – What Should You Spend Your Money On? Keith Buzzard, Computers and Security V18 (1999) pp322-334